

# Supported TLS cipher suites

Published: 2024-09-03

The ExtraHop system can decrypt TLS traffic that has been encrypted with PFS or RSA cipher suites. All supported cipher suites can be decrypted by installing the session key forwarder on a server and configuring the ExtraHop system.

Cipher suites for RSA can also decrypt the traffic with a certificate and private key—with or without session key forwarding.

## Decryption methods

The table below provides a list of cipher suites that the ExtraHop system can **decrypt** along with the supported decryption options.

- **PFS + GPP:** the ExtraHop system can decrypt these cipher suites with session key forwarding and **global protocol to port mapping**
- **PFS + Cert:** the ExtraHop system can decrypt these cipher suites with session key forwarding and the **certificate and private key**
- **RSA + Cert:** the ExtraHop system can decrypt these cipher suites without session key forwarding as long as you have uploaded the **certificate and private key**

| Hex Value | Name (IANA)                       | Name (OpenSSL)       | Supported Decryption            |
|-----------|-----------------------------------|----------------------|---------------------------------|
| 0x04      | TLS_RSA_WITH_RC4_128_MD5          | RC4-MD5              | PFS + GPP PFS + Cert RSA + Cert |
| 0x05      | TLS_RSA_WITH_RC4_128_SHA          | RC4-SHA              | PFS + GPP PFS + Cert RSA + Cert |
| 0x0A      | TLS_RSA_WITH_3DES_EDE_CBC_SHA     | DES-CBC3-SHA         | PFS + GPP PFS + Cert RSA + Cert |
| 0x16      | TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA | EDH-RSA-DES-CBC3-SHA | PFS + GPP PFS + Cert            |
| 0x2F      | TLS_RSA_WITH_AES_128_CBC_SHA      | AES128-SHA           | PFS + GPP PFS + Cert RSA + Cert |
| 0x33      | TLS_DHE_RSA_WITH_AES_128_CBC_SHA  | DHE-RSA-AES128-SHA   | PFS + GPP PFS + Cert            |
| 0x35      | TLS_RSA_WITH_AES_256_CBC_SHA      | AES256-SHA           | PFS + GPP PFS + Cert RSA + Cert |
| 0x39      | TLS_DHE_RSA_WITH_AES_256_CBC_SHA  | DHE-RSA-AES256-SHA   | PFS + GPP PFS + Cert            |
| 0x3C      | TLS_RSA_WITH_AES_128_CBC_SHA256   | AES128-SHA256        | PFS + GPP PFS + Cert RSA + Cert |

| Hex Value | Name (IANA)                             | Name (OpenSSL)               | Supported Decryption            |
|-----------|-----------------------------------------|------------------------------|---------------------------------|
| 0x3D      | TLS_RSA_WITH_AES_256_CBC_SHA256         | AES256-SHA256                | PFS + GPP PFS + Cert RSA + Cert |
| 0x67      | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256     | DHE-RSA-AES128-SHA256        | PFS + GPP PFS + Cert            |
| 0x6B      | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256     | DHE-RSA-AES256-SHA256        | PFS + GPP PFS + Cert            |
| 0x9C      | TLS_RSA_WITH_AES_128_GCM_SHA256         | AES128-GCM-SHA256            | PFS + GPP PFS + Cert RSA + Cert |
| 0x9D      | TLS_RSA_WITH_AES_256_GCM_SHA384         | AES256-GCM-SHA384            | PFS + GPP PFS + Cert RSA + Cert |
| 0x9E      | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256     | DHE-RSA-AES128-GCM-SHA256    | PFS + GPP PFS + Cert            |
| 0x9F      | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384     | DHE-RSA-AES256-GCM-SHA384    | PFS + GPP PFS + Cert            |
| 0x1301    | TLS_AES_128_GCM_SHA256                  | TLS_AES_128_GCM_SHA256       | PFS + GPP PFS + Cert            |
| 0x1302    | TLS_AES_256_GCM_SHA384                  | TLS_AES_256_GCM_SHA384       | PFS + GPP PFS + Cert            |
| 0x1303    | TLS_CHACHA20_POLY1305_SHA256            | TLS_CHACHA20_POLY1305_SHA256 | PFS + GPP PFS + Cert            |
| 0xC007    | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        | ECDHE-ECDSA-RC4-SHA          | PFS + GPP                       |
| 0xC008    | TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA   | ECDHE-ECDSA-DES-CBC3-SHA     | PFS + GPP                       |
| 0xC009    | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA    | ECDHE-ECDSA-AES128-SHA       | PFS + GPP                       |
| 0xC00A    | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA    | ECDHE-ECDSA-AES256-SHA       | PFS + GPP                       |
| 0xC011    | TLS_ECDHE_RSA_WITH_RC4_128_SHA          | ECDHE-RSA-RC4-SHA            | PFS + GPP PFS + Cert            |
| 0xC012    | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA     | ECDHE-RSA-DES-CBC3-SHA       | PFS + GPP PFS + Cert            |
| 0xC013    | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA      | ECDHE-RSA-AES128-SHA         | PFS + GPP PFS + Cert            |
| 0xC014    | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      | ECDHE-RSA-AES256-SHA         | PFS + GPP PFS + Cert            |
| 0xC023    | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | ECDHE-ECDSA-AES128-SHA256    | PFS + GPP                       |

| Hex Value | Name (IANA)                                   | Name (OpenSSL)                | Supported Decryption |
|-----------|-----------------------------------------------|-------------------------------|----------------------|
| 0xC024    | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384       | ECDHE-ECDSA-AES256-SHA384     | PFS + GPP            |
| 0xC027    | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256         | ECDHE-RSA-AES128-SHA256       | PFS + GPP PFS + Cert |
| 0xC028    | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384         | ECDHE-RSA-AES256-SHA384       | PFS + GPP PFS + Cert |
| 0xC02B    | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256       | ECDHE-ECDSA-AES128-GCM-SHA256 | PFS + GPP            |
| 0xC02C    | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384       | ECDHE-ECDSA-AES256-GCM-SHA384 | PFS + GPP            |
| 0xC02F    | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256         | ECDHE-RSA-AES128-GCM-SHA256   | PFS + GPP PFS + Cert |
| 0xC030    | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384         | ECDHE-RSA-AES256-GCM-SHA384   | PFS + GPP PFS + Cert |
| 0xCCA8    | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256   | ECDHE-RSA-CHACHA20-POLY1305   | PFS + GPP PFS + Cert |
| 0xCCA9    | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 | ECDHE-ECDSA-CHACHA20-POLY1305 | PFS + GPP            |
| 0xCCAA    | TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256     | DHE-RSA-CHACHA20-POLY1305     | PFS + GPP PFS + Cert |